

JD:VTN
F.#2018R00005

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
ONE SAMSUNG CELLULAR DEVICE,
MODEL G550T, IMEI NUMBER
353764/08/279033/2

APPLICATION FOR A SEARCH
WARRANT FOR AN ELECTRONIC
DEVICE

Case No. **18M260**

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Tyler Miceli, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco and Firearms (“ATF”) and have been for approximately two and a half years. I have extensive experience in conducting robbery and fugitive investigations. As a result of my training and experience, I am familiar with the practice of searching for and obtaining electronic evidence to help identify, locate and prosecute defendants. I have participated in dozens of investigations involving search warrants, including warrants for the search of electronic devices.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from my personal participation in this investigation and reports by other law enforcement authorities. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Based on the facts set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence and instrumentalities of violations of a Hobbs Act Robbery, in violation of Title 18, United States Code, Section 1951, and possessing, brandishing and discharging a firearm during a crime of violence, in violation of Title 18, United States Code, Sections 924(c)(1)(A)(i), 924(c)(1)(A)(ii) and 924(c)(1)(A)(iii).

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is one Samsung cellular device, model G550T, IMEI number 353764/08/279033/2, hereinafter the "Device." The Device is currently in the custody of the Bureau of Alcohol, Tobacco and Firearms within the Eastern District of New York.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On March 22, 2018, in the Eastern District of New York, Steven Enrique was arraigned on an indictment (18-CR-0122) charging him with a Hobbs Act Robbery, in violation of Title 18, United States Code, Section 1951, and possessing, brandishing and discharging a firearm during a crime of violence, in violation of Title 18, United States Code, Sections 924(c)(1)(A)(i), 924(c)(1)(A)(ii) and 924(c)(1)(A)(iii).

8. On March 22, 2018, Jamel Robinson was placed under arrest pursuant to an arrest warrant (18-M-206) issued on March 7, 2018, by the Honorable Robert M. Levy, United States Magistrate Judge for the Eastern District of New York, for a Hobbs Act Robbery, in violation of Title 18, United States Code, Section 1951, and possessing, brandishing and discharging a firearm during a crime of violence, in violation of Title 18, United States Code, Sections 924(c)(1)(A)(i), 924(c)(1)(A)(ii) and 924(c)(1)(A)(iii).

9. The charges against Enrique and Robinson are based on a theory of acting in concert for an armed robbery that occurred on December 19, 2017. Enrique acted as a lookout for Robinson before Robinson entered a grocery store at 707 Fulton Street in Brooklyn, New York. Upon entering the store, Robinson went to the cashier, brandished a pistol, demanded money, and shot the cashier in the foot. The cashier opened a cash register and Robinson removed approximately \$2,000 cash from the tray, and exited the store.

10. During the course of my investigation of the crime, I reviewed surveillance video of the robbery and from the surrounding areas of 707 Fulton Street. I observed that approximately 15 minutes prior to the robbery, Enrique was seated on a stoop in front of a

building on St. Felix Street, between Fulton Street and Dekalb Avenue for several minutes before Robinson approached and began speaking to Enrique. After the two men spoke with one another for about a minute, Enrique proceeded south on St. Felix Street, toward Fulton Street, ahead of Robinson. Robinson then proceeded in the same direction. I further observed on video that in the minutes preceding the robbery, Enrique was standing alone in front of the store at 707 Fulton Street for more than five minutes, watching as customers exited the store, and looking westward before he finally entered the store. Seconds before Enrique entered the store, Robinson appeared from the west side of Fulton Street and entered the store shortly after Enrique.

11. While Enrique was inside the store, he pretended to be a customer and watched as Robinson shot the cashier and left the store with the money. Enrique then called 911 from his cell phone to report the robbery. The 911 call made by Enrique was from cell phone number (718) 809-0917. I have reviewed call detail records provided by Sprint, the service provider for said phone number, and determined that between December 7, 2017 and December 30, 2017, there were approximately 458 communications between Enrique's phone number and phone number (631) 640-7758, and that more than half of those communications were text message exchanges that occurred on December 19, 2017.

12. I believe that phone number (631) 640-7758 was being used by Robinson on or about December 19, 2017, and at other times. Specifically, on or about January 29, 2018, a woman named Tyisha Reid went to the 88th Precinct in Brooklyn, New York to report an unrelated crime. Ms. Reid reported that she is the wife of Jamel Robinson and that his phone

number is (631) 640-7758. Call detail records received from T-Mobile US, Inc., the service provider for said phone number, for the period of December 1, 2017 through January 8, 2018, reveal approximately 150 communications between (631) 640-7758 and the cell phone number which Ms. Reid said was her own personal phone number.

13. ATF obtained authorization to use a cell-site simulator to locate the cellular device assigned call number (631) 640-7758, and on March 22, 2018, law enforcement used a cell-site simulator to track the cellular device believed to be used Robinson to the vicinity of Clarkson Avenue and 54th Street in Brooklyn, New York. Upon arriving to that location, a law enforcement officer recognized Robinson and placed him under arrest. Upon a search of Robinson on March 22, 2018, he had in his possession a Samsung cellular device, model G550T, IMEI number 353764/08/279033/2. The Device was recovered from Robinson upon his arrest and is currently in the lawful possession of the ATF within the Eastern District of New York.

14. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the ATF.

TECHNICAL TERMS

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard

drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by

radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g.,

121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

16. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data

stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

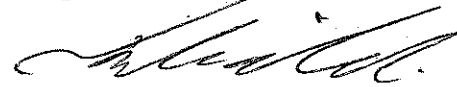
19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

21. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



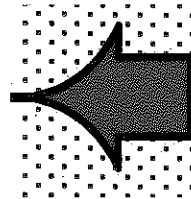
Tyler Miceli
Special Agent
Bureau of Alcohol, Tobacco and Firearms

Subsc
on Ma



THE
UNIT
EAST

GOLD
JUDGE
ORK



ATTACHMENT A

The property to be searched is a Samsung cellular device, model G550T, IMEI number 353764/08/279033/2, hereinafter the “Device.” The Device is currently in the custody of the Bureau of Alcohol, Tobacco and Firearms within the Eastern District of New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code, Sections 1951, 924(c)(1)(A)(i), 924(c)(1)(A)(ii) and 924(c)(1)(A)(iii) and involve Jamel Robinson and his co-conspirator(s) since December 7, 2017, including:
 - a. all records and information on the Device, including names and telephone numbers, as well as the contents of all call logs, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook or other social media posts or messages, Internet activity (including browser history, web page logs and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of the above-listed offenses;
 - b. all contact lists;
 - c. any information recording the whereabouts of Jamel Robinson and his co-conspirator(s) on December 19, 2017;
 - d. all bank records, checks, credit card bills, account information, and other financial records from on or after December 19, 2017;
 - e. passwords, encryption keys and other access devices that may be necessary to access the Devices; and

- f. contextual information necessary to understand the evidence described in this attachment.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.